Robust Trust Management

(Doctoral Consortium)

Athirai A. Irissappane
School of Computer Engineering
Nanyang Technological University, Singapore
athirai001@e.ntu.edu.sg

1. RESEARCH PROBLEM

Our research is within the area of artificial intelligence and multi-agent systems. More specifically, we focus on the robustness issues [1] in reputation systems for electronic marketplaces and aim to address the following problems,

- how to cope with dishonest advisors (buyers who provide misleading opinions), improving the robustness of the trust model.
- how to choose an appropriate seller to perform transaction by querying advisors in an optimal way.

To explain, in multi-agent based e-marketplaces, self-interested selling agents may act maliciously by not delivering products with the same quality as promised. It is thus important for buying agents to analyze their quality and determine which sellers to do business with, based on their previous experience with the sellers. However, realistically, in most e-marketplaces, buyers often encounter sellers with which they have no previous experience. In such cases, they can query other buyers (called advisors) about the sellers. But, advisors may act dishonestly by providing misleading opinions (unfair ratings) to promote low quality sellers or demote sellers with high quality. Hence, it is necessary to evaluate the quality of advisors' opinions to determine their reliability.

While it is prima facie necessary to gather opinions about a seller, a buyer may not need to query all the advisors about the seller, since the cost of querying all the advisors may be greater than the value derived from a successful transaction with the seller. Thereby, it is necessary to design an optimal scheme to selectively query advisors and choose a quality seller to perform transaction, in order to maximize the utility of the buyer in the long run.

2. PROGRESS TO DATE

Up to date we have proposed: 1) a biclustering based approach to identify dishonest advisors in a multi-criteria e-marketplace; 2) a POMDP based approach (called the SALE POMDP) to optimally select sellers in an e-marketplace.

2.1 The Biclustering Based Approach

Existing trust models [2, 3] such as BRS, iCLUB, etc., which deal with the unfair rating problem are only designed to operate in a single-criterion environment and cannot effectively cope with sophisticated attacks in a multi-criteria scenario (seller is evaluated on multiple criteria). Few trust models [4] have also been proposed for handling multi-criteria ratings. However, they do not address the problem of unfair ratings.

We have proposed a novel approach to filter dishonest advisors, specific to a multi-criteria scenario by adopting a biclustering mechanism [5] to cluster advisors, honest to a subset of criteria. Such a mechanism effectively identifies dishonest advisors, who provide honest ratings to some criteria, while acting malicious on others.

Every active buyer b (i.e. the buyer evaluating the current seller) is assigned a set of biclusters, each of which consists of the active buyer, advisors and criteria for which the advisors are identified honest. Specifically, to form a bicluster, we begin with an initial bicluster, containing buyer b and several randomly chosen criteria. We iteratively add (delete) advisors and criteria from the bicluster such that distance of the advisors from the mean is smaller (larger) than a threshold and advisors have similar (different) criteria correlation as b. We iterate until convergence to obtain the final bicluster. Different subsets of criteria are considered in the initial bicluster to obtain different biclusters for buyer b. The biclusters are again scanned for possible malicious advisors by employing the majority rule, to cope with extreme attacking scenarios. The confidence in trusting advisors is then computed such that advisors belonging to biclusters with many criteria are given more weights and advisors not belonging to any bicluster are considered dishonest and filtered.

There are two important features considered in the biclustering process: 1) rating correlation between criteria is used as additional information to detect sophisticated dishonest advisors, honest to all sellers but the current seller, when the active buyer has no personal experience with the current seller; 2) trust transitivity is exploited by deciding a proper order for advisors to be added to bicluster. This feature is especially useful to identify dishonest advisors in sparse scenarios. Evaluation in a simulated e-marketplace environment shows that our approach is robust in effectively filtering dishonest advisors even in the presence of sophisticated unfair rating attacks (constant, camouflage, whitewashing and sybil attacks), obtaining a better MCC [5] than BRS and iCLUB.

2.2 The SALE-POMDP Model

Existing trust models [2, 3] mainly focus on accurately estimating the quality of sellers rather than optimally choosing a good seller to perform transaction; they simply query *all* advisors about the sellers' quality and fail to reason *when* it is really necessary to query advisors (about the sellers' quality).

We propose the SALE *(S)eller & (A)dvisor se(LE)ction* POMDP, a novel POMDP based framework to deal with the seller selection problem that overcomes the above problem by reasoning about advisor trustworthiness and selectively querying for information [6].

Appears in: *Alessio Lomuscio, Paul Scerri, Ana Bazzan, and Michael Huhns (eds.), Proceedings of the 13th International Conference on Autonomous Agents and Multiagent Systems (AAMAS 2014), May 5-9, 2014, Paris, France.*

POMDPs provide a natural model for sequential decision making under uncertainty. The main advantage that the POMDP scheme brings to the seller selection problem is that it enables optimal trade-off of the expected benefit and cost of obtaining more information, aiming to maximize the total utility of the buyer.

Given I advisors that can be queried about the quality of J sellers, each SALE POMDP agent can be described in terms of states, actions, observations and rewards as follows.

States. A state contains the quality levels of each seller ($high, low$), each advisor ($trustworthy, adversarial, random$) and the status of the transaction with the seller ($not\_started$, $satisfactory$, $unsatisfactory$, $gave\_up$, $finished$).

Actions. The model knows the following types of actions: 1) $seller\_query_{ij}(SQ_{ij})$, ask advisor i about quality of seller j; 2) $advisor\_query_{ii'}$ ($AQ_{ii'}$), ask advisor i about quality of advisor i'; 3) buy_j, buy from seller j; 3) do_not_buy (DNB), decide not to buy from any seller in the market.

Transitions. We assume that when taking a query action, the state does not change. When taking buy_j and DNB actions, the state will always transition to a terminal state, i.e., buy_j actions may result in a successful (sat = $satisfactory$) or unsuccessful ($sat = unsatisfactory$) transaction and DNB will result in $sat = gave\_up$. Transition probabilities to terminal states give the *definition* of quality levels. Generally, chances of transition to $satisfactory$ should be high on buying from 'high quality' sellers.

Rewards. There is small cost for the ask actions. A reward is associated with a successful transaction, otherwise a penalty is levied. There is a penalty for taking DNB action, when in fact there is a seller of high quality, otherwise there is a reward for this action. Once the terminal states are reached, no further rewards are given.

Observations. When a *query* action is performed, the agent will receive an observation based on the set of discriminated quality levels. After SQ_{ij} action, the agent receives an observation $o \in \{good, bad\}$, corresponding to the quality of seller j. After $AQ_{ii'}$ action, it gets an observation $o \in \{trustworthy, untrustworthy\}$, corresponding to the quality of advisor i'. On transition to a terminal state, it receives the observation $ended$.

Observation Function. It specifies the likelihood of receiving an observation given the current state and the action that led to this state. There is no a priori correct way to specify the observation probabilities. Similar to the transition probabilities for buy action, probabilities for the observation function *define* the meaning of different trust levels. In general, the idea is that trustworthy advisors give more accurate and consistent answers than untrustworthy ones.

Initial State Distribution. We assume a uniform belief over the quality levels, but a different initial belief can also be obtained as a result of previous interactions. We will also assume an infinite horizon problem.

The SALE POMDP model works by improving its beliefs over the quality levels of sellers and advisors by querying advisors about the quality of sellers/other advisors in the system, until it is sure that it has identified a seller with sufficient quality. If $b(s)$ specifies the probability of a state s (for all s), we can derive b' an updated belief after taking action a and receiving observation o using Bayes' rule,

$$b'(s') = \frac{\Pr(s', o|b, a)}{\Pr(o|b, a)} = \frac{\Pr(o|a, s')}{\Pr(o|b, a)} \sum_s Pr(s'|s, a)b(s) \quad (1)$$

Also, the belief updates are performed such that they correlate the state factors in meaningful ways, e.g., observing $good$ after $seller\_query_{ij}$ will give more weights to states where the seller is $high$ quality and the advisor is $trustworthy$, and less weights to states where the seller is low quality. We also represent the SALE POMDP in factored form to improve its scalability and use symbolic Perseus [6] as the POMDP solver for the experiments. Extensive evaluation on the ART testbed demonstrates that SALE POMDP balances the cost of obtaining and benefit of more information more effectively, leading to more earnings, than traditional trust models. Experiments also show that it is more robust to deceptive advisors than a previous POMDP based approach.

3. FUTURE WORK

For the future work, we plan to extend our current trust models, improving their robustness and enhancing their applicability to different real-world scenarios. More specifically, the current biclustering based approach works well, if the users assign equal importance to the various evaluation criteria. However, in real-world, users may have different subjectivity for evaluation. In this case, we will extend our approach by considering the importance of different criteria. Also, in real-world, users may not provide ratings to all the criteria, every time. We will deal with such scenarios, by using correlation information between criteria, to predict the ratings for the missing criteria. Also, we plan to improve the complexity of the biclustering approach using approximation strategies, e.g., random initialization of bicluster members.

Our current SALE POMDP model optimally selects sellers by modeling seller and advisor trustworthiness on a single-criterion. We will extend the model to a multi-criteria scenario, where a seller is selected based on its trustworthiness on a number of criteria. We will also include more detailed advisor models (e.g., differentiating its trustworthiness in providing opinions about sellers and other advisors) to improve the robustness of the approach.

We also consider to apply the SALE POMDP model to the routing problem in wireless sensor networks. Here, the SALE POMDP agent will select a suitable (trustworthy) sensor node to route packets. The neighboring sensor nodes will be assigned beliefs based on their ability to route packet data (based on multiple-criteria). The SALE POMDP agent will work by improving its beliefs over the quality levels of its neighbors by querying information until it has identified a suitable neighboring sensor to route packets. The optimal policy suggested by the SALE POMDP model will balance the expected benefit of obtaining more information about the sensor nodes against the cost (in terms of energy consumption) of obtaining this information.

4. REFERENCES

[1] Irissappane, Athirai A., Jiang, Siwei, Zhang, Jie: A testbed to evaluate the robustness of reputation systems in e-marketplaces. In AAMAS, 2014.

[2] Jøsang, A., Ismail, R., Boyd, C.: A survey of trust and reputation systems for online service provision. Decision support systems, 43(2), 618–644, 2007.

[3] Irissappane, Athirai A., Jiang, Siwei, Zhang, Jie: A framework to choose trust models for different e-marketplace environments. In IJCAI, 2013.

[4] Reece, S., Rogers, A., Roberts, S., Jennings, N.R.: Rumours and reputation: Evaluating multi-dimensional trust within a decentralised reputation system. In AAMAS, 2007.

[5] Irissappane, Athirai A., Jiang, Siwei, Zhang, Jie: A biclustering-based approach to filter dishonest advisors in multi-criteria e-marketplaces. In AAMAS, 2014.

[6] Irissappane, Athirai A., Oliehoek, Frans A., Zhang, Jie: A POMDP based approach to optimally select sellers in electronic marketplaces. In AAMAS, 2014.